Améliorer la sécurité, la confidentialité et l’anonymat de votre smartphone

Michel NALLINO

Nice, France, 2026-09-23 – Révision 19

Copyright Michel NALLINO 2025 – 2026.

Cette œuvre est distribuée sous la licence Creative Commons, Attribution-NonCommercial 4.0 International (CC BY-NC 4.0), voir https://creativecommons.org/licenses/by-nc/4.0/

Clause de non-responsabilité :

IL N’Y A AUCUNE GARANTIE POUR LE CONTENU DU DOCUMENT, DANS LA MESURE PERMISE PAR LA LOI APPLICABLE.

LE TITULAIRE DU DROIT D’AUTEUR FOURNIT LE CONTENU DU DOCUMENT TEL QUEL, SANS GARANTIE D’AUCUNE SORTE, EXPRIMÉE OU IMPLICITE, Y COMPRIS, MAIS SANS S’Y LIMITER, LES GARANTIES IMPLICITES DE QUALITÉ MARCHANDE ET D’ADÉQUATION DANS UN BUT PARTICULIER.

VOUS ASSUMEZ LA TOTALITÉ DES RISQUES EN UTILISANT LE CONTENU DU DOCUMENT. SI LE CONTENU DU DOCUMENT SE RÉVÈLE FAUX, VOUS ASSUMEZ LE COÛT DE TOUS LES ENTRETIENS, RÉPARATIONS OU CORRECTIONS NÉCESSAIRES.

Liens internes au document

1. Introduction
2. Résolveurs DNS filtrants
    - 2.1) Cloudflare avec filtrage des maliciels
    - 2.2) Cloudflare avec filtrage des maliciels et du contenu pour adultes
    - 2.3) OpenDNS Protection familiale
    - 2.4) Résolveur DNS configurable de Rethink
    - 2.5) Résolveur DNS configurable uBlockDNS
    - 2.6) Résolveurs DNS souverains et conformes au RGPD pour les citoyens de l’UE
3. Smartphones Android
    - 3.1) Introduction à Android
    - 3.2) Utilisation de distributions alternatives
        - Distributions Linux
            - Ubuntu Touch
            - Sailfish OS
            - PostmarketOS
            - Mobian
            - Plasma Mobile
            - PureOS
        - Distributions Android alternatives
            - /e/OS
            - LineageOS
            - iodéOS
            - GrapheneOS
            - Huawei
            - XDA Developers
    - 3.3) Utilisation des smartphones Android du commerce
        - Protection contre les logiciels malveillants, les pisteurs et la publicité.
        - Libération partielle de Google

Choix du navigateur

Un zoom sur Firefox et Cromite

Autres précautions

VPN

Anonymat

4. iPhones

4.1) Introduction aux iPhones

4.2) Protection contre les maliciels, la publicité et le pistage dans iOS

Autres précautions pour iOS

VPN sur iOS

Anonymat sur iOS

1. Introduction

Les smartphones ont envahi nos vies, au point qu'ils apparaissent parfois comme absolument nécessaires. Cependant, bien que pratiques, ils sont souvent perçus comme des « espions dans la poche », au point que certaines personnes refusent de les utiliser.

L'objectif de ce petit guide est de montrer comment améliorer la sécurité, la confidentialité et l'anonymat de votre smartphone, quel que soit le type de votre appareil, de votre smartphone Android ou de votre iPhone Apple.

Quelques chiffres : Il y a aujourd'hui ~ 8,6 milliards de smartphones utilisés dans le monde par ~ 7,3 milliards d'utilisateurs. Les smartphones Android actifs sont de ~ 5,4 à 5,6 milliards, et les iPhones actifs représentent plus d'un milliard.

2. Résolveurs DNS filtrants

Les résolveurs DNS filtrants sont des outils communs aux smartphones Android et aux iPhones pour augmenter leur sécurité et leur confidentialité.

Ainsi, ce chapitre est valable pour les deux types d'appareils, et la façon de les utiliser sera expliquée dans les chapitres dédiés correspondants.

2.1) Cloudflare avec filtrage des maliciels :

Adresse IPV4 du serveur primaire : 1.1.1.2

Adresse IPV4 du serveur secondaire : 1.0.0.2

Adresse IPV6 du serveur primaire : 2606:4700:4700::1112

Adresse IPV6 du serveur secondaire : 2606:4700:4700::1002

DNS over HTTPS: https://security.cloudflare-dns.com/dns-query

DNS over TLS: security.cloudflare-dns.com

2.2) Cloudflare avec filtrage des maliciels et du contenu pour adultes :

Adresse IPV4 du serveur primaire : 1.1.1.3

Adresse IPV4 du serveur secondaire : 1.0.0.3

Adresse IPV6 du serveur primaire : 2606:4700:4700::1113

Adresse IPV6 du serveur secondaire : 2606:4700:4700::1003

DNS over HTTPS: https://family.cloudflare-dns.com/dns-query

DNS over TLS: family.cloudflare-dns.com

2.3) OpenDNS Protection familiale :

Adresse IPV4 du serveur primaire : 208.67.222.123

Adresse IPV4 du serveur secondaire : 208.67.220.123

Adresse IPV6 du serveur primaire : 2620:119:35::123

Adresse IPV6 du serveur secondaire 2620:119:53::123

DNS over HTTPS: https://doh.familyshield.opendns.com/dns-query

DNS over TLS: familyshield.opendns.com

[NB : Cisco a arrêté les activités d'OpenDNS en France, en vigueur depuis le 28 juin 2024. Voir :

https://support.opendns.com/hc/en-us/articles/27951404269204-OpenDNS-Service-Not-Available-To-Users-In-France-and-Portugal (le service a depuis été réactivé au Portugal).]

2.4) Résolveur DNS configurable de Rethink :

Rethink propose, gratuitement pour le moment, un résolveur DNS filtrant configurable :

– le filtrage, selon votre choix, s'effectue sur les serveurs rethinkdns.com,

– les requêtes DNS sont ensuite envoyées par Rethink à un réseau de résolveurs DNS (Cloudflare etc.) .

Il y a deux façons de configurer le filtrage :

* configuration « avancée », sur https://rethinkdns.com/configure, vous sélectionnez les filtres que vous voulez dans une liste de plus de 190 ;

* configuration « simple », à partir de la page Web précédente, vous cliquez sur le bouton « Simple », et vous sélectionnez des catégories complètes de filtres (Adult, Piracy, Gambling, Dating, Social Media, Security Full, Security Extra, Privacy Lite, Privacy Aggressive, Privacy Extreme).

Dans les deux cas, une fois votre sélection terminée, vous obtenez un nom de résolveur DNS en tant que DNS over TLS (DoT) ou DNS over HTTPS (DoH).

Exemple : après avoir sélectionné parmi la page de configuration simple Security Full et Privacy Aggressive, vous obtenez le nom de résolveur DNS suivant, en tant que DoT :

« 1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com ».

On peut aussi installer l'application « Rethink: DNS + Pare-feu + VPN » et tout gérer depuis l'application

[NB : au 21/05/2026, Rethink n'offre pas la possibilité d'une liste blanche de sites.]

2.5) Résolveur DNS configurable uBlockDNS :

Ce résolveur fonctionne de manière similaire à Rethink :

– le filtrage, selon votre choix, s'effectue sur les serveurs ublockdns.com,

– les requêtes DNS, selon votre choix, sont ensuite envoyées sur AdGuard DNS, Cloudfare, Google Public DNS ou Quad9.

Vous allez sur https://ublockdns.com/, vous cliquez sur « Get Started » et vous obtenez une clé (4 petits mots anglais) que vous enregistrez. Aucune adresse e-mail n'est requise, ni nom d'utilisateur.

Ensuite vous sélectionnez votre profil (Standard, Famille, Strict), puis sélectionnez éventuellement des listes de filtrage supplémentaires, et votre profil DNS (Automatique, Focus sur la confidentialité, Focus sur la sécurité, Focus sur les performances ou Focus sur le filtrage).

Vous obtenez un serveur DNS DoT : « xxxxxxxx.dot.ublockdns.com »,
et un DoH : « https://my.ublockdns.com/xxxxxxxx ».
Le nom « xxxxxxx » est unique, et attaché à la clé de quatre mots.

2.6) Résolveurs DNS souverains et conformes au RGPD pour les citoyens de l'UE:

Il existe des résolveurs DNS souverains, conformes au RGPD :

– « Souverains » : les serveurs sont à l'intérieur de l'UE, et il y a au moins un serveur dans chacun des 27 pays de l'UE,

– « Conformes au RGPD »: offrant la meilleure protection contre la confidentialité à ses utilisateurs, conformément à la réglementation générale de la protection des données de l'UE, voir https://gdpr-info.eu/,

– « Compatibles DNSSEC »: les réponses DNS sont signées par les serveurs.

Ils sont gérés par DNS4EU, projet financé par l'UE, voir https://www.joindns4.eu/. Ces résolveurs DNS existent en cinq versions :

Nom d'hôte	**Publicité**	**Pisteurs**	**Maliciels**	**Adultes**
unfiltered.joindns4.eu				
protective.joindns4.eu			✅	
noads.joindns4.eu	✅	✅	✅	
child.joindns4.eu			✅	✅
child-noads.joindns4.eu	✅	✅	✅	✅

Résolveur DNS non filtrant :

Adresse IPV4 du serveur primaire : 86.54.11.100

Adresse IPV4 du serveur secondaire : 86.54.11.200

Adresse IPV6 du serveur primaire : 2a13:1001::86:54:11:100

Adresse IPV6 du serveur secondaire : 2a13:1001::86:54:11:200

DNS over HTTPS: https://unfiltered.joindns4.eu/dns-query

DNS over TLS: unfiltered.joindns4.eu

Résolveur DNS protecteur :

Ce résolveur DNS est durci, orienté sécurité.

Adresse IPV4 du serveur primaire : 86.54.11.1

Adresse IPV4 du serveur secondaire : 86.54.11.201

Adresse IPV6 du serveur primaire : 2a13:1001::86:54:11:1

Adresse IPV6 du serveur secondaire : 2a13:1001::86:54:11:201

DNS over HTTPS: https://protective.joindns4.eu/dns-query

DNS over TLS: protective.joindns4.eu

Résolveur DNS protecteur et filtrant la publicité :

Adresse IPV4 du serveur primaire : 86.54.11.13

Adresse IPV4 du serveur secondaire : 86.54.11.213

Adresse IPV6 du serveur primaire : 2a13:1001::86:54:11:13

Adresse IPV6 du serveur secondaire : 2a13:1001::86:54:11:213

DNS over HTTPS: https://noads.joindns4.eu/dns-query

DNS over TLS: noads.joindns4.eu

Résolveur DNS protecteur avec filtrage du contenu pour adultes :

Adresse IPV4 du serveur primaire : 86.54.11.12

Adresse IPV4 du serveur secondaire : 86.54.11.212

Adresse IPV6 du serveur primaire : 2a13:1001::86:54:11:12

Adresse IPV6 du serveur secondaire : 2a13:1001::86:54:11:212

DNS over HTTPS: https://child.joindns4.eu/dns-query

DNS over TLS: child.joindns4.eu

Résolveur DNS protecteur avec filtrage du contenu pour adultes et de la publicité :

Adresse IPV4 du serveur primaire : 86.54.11.11

Adresse IPV4 du serveur secondaire : 86.54.11.211

Adresse IPV6 du serveur primaire : 2a13:1001::86:54:11:11

Adresse IPV6 du serveur secondaire : 2a13:1001::86:54:11:211

DNS over HTTPS: https:/child-noads.joindns4.eu/dns-query/

DNS over TLS: child-noads.joindns4.eu

3. Smartphones Android

3.1) Introduction à Android

Les appareils Android incluent un système d'exploitation avec plusieurs couches :

– Un noyau Linux, personnalisé pour Android.

– Une couche d'Open Source Android, AOSP, voir https://source.android.com/.

– Dans la plupart des cas, une couche Google (avec Google Play, Google Play Service, Google Assistant ou Gemini, Android Auto, Google Chrome, Gmail, Google Maps, etc.).

– Des pilotes et des réglages spécifiques au fabricant.

– Dans certains cas, une couche de fabricant supplémentaire (exemple, Samsung) sur celle de Google ou remplaçant partiellement certaines applications Google.

– Applications installées à partir de Google Play Store ou de magasins alternatifs tels que Accrescent, Aurora, F- Droid, Obtainium... ou installées à partir d'un fichier apk.

[NB : Google entend restreindre la possibilité d'installer des applications sous forme d'apks ou provenant d'un autre magasin que le sien, voir https://keepandroidopen.org/].

La sécurité d'Android repose sur l'utilisation d'un bac à sable fort SELinux (Security Enhanced Linux) + seccompbpf, au niveau du noyau, qui assure une isolation complète des applications. Chaque application s'exécute avec son identification d'utilisateur unique, les applications n'ont pas accès aux répertoires système ou aux répertoires d'autres applications. Des autorisations sont nécessaires (notifications, accès aux capteurs, envoi de données en arrière-plan, utilisation de la batterie, etc.) ; elles sont définies par défaut, mais l'utilisateur peut les modifier. Certains mécanismes permettent un partage de données et de fichiers entre des applications en bac à sable.

Les connexions entrantes sont bloquées (un pare-feu supplémentaire n'aurait d'intérêt que pour bloquer des connexions sortantes, et installer un serveur nécessiterait de rooter l'appareil).

Les failles de sécurité viennent essentiellement de l'installation et de l'usage de maliciels. Les logiciels malveillants sont contrôlés par Google dans son Play Store et par Google Security sur l'appareil. Le contrôle des logiciels malveillants pas Google n'est pas parfait, régulièrement des maliciels sont rendus disponibles dans Play Store. Le risque de télécharger et d'installer des logiciels malveillants est plus élevé lors de l'utilisation de magasins alternatifs ou lors de l'installation à partir d'un fichier APK.

Il est recommandé d'arrêter et de redémarrer périodiquement les périphériques Android, pour supprimer les maliciels persistant en mémoire.

Comme pour tout système d'exploitation, il est recommandé de le mettre à jour le plus souvent possible (système et applications), pour les corrections de bogues et les correctifs de sécurité.

Le principal problème avec Android est le pistage : vous êtes traqué par Google et par toutes les applications « gratuites » (non payantes) installées sur l'appareil (et même par certaines applications payantes).

Les publicités sont un autre problème, affichées parfois si agressivement à l'intérieur des applications qu'elles empêchent leur utilisation normale.

3.2) Utilisation de distributions alternatives

Certains utilisateurs peuvent installer des distributions alternatives à la place celles livrées avec leur smartphone Android, afin d'être complètement libérés de Google.

Cela nécessite une compétence de l'utilisateur, et ce n'est pas disponible pour tous les appareils.

L’installation d’une distribution alternative est risquée : une mauvaise manipulation pourrait rendre inutilisable le smartphone. Ce risque est annulé lorsque l’utilisateur achète un smartphone avec l’une de ces distributions préinstallées.

Ces distributions alternatives concernent un nombre limité d’appareils, pour lesquels les sources des pilotes sont disponibles.

Enfin, sans compte Google, la sauvegarde Google Cloud n’est pas possible ; l’utilisateur doit configurer une autre solution de sauvegarde et restauration. Certains utilisateurs choisissent une sauvegarde RSYNC en mode racine, mais certaines applications telles que Netflix ne fonctionneront pas une fois le smartphone en mode racine.

→ **Pour toutes ces raisons, c’est une utilisation de niche.**

Voici quelques distributions alternatives :

Distributions Linux :

* Ubuntu Touch

https://www.ubuntu-touch.io/

« Une expérience complète d’un système d’exploitation mobile, qui est le vôtre ».

Ubuntu Touch est un système d’exploitation Linux, dédié aux smartphones, remplaçant totalement Android.

Il est compatible avec la liste des appareils suivants : https://devices.ubuntu-touch.io/. il est possible de l’obtenir préinstallé sur certains appareils (Volla, Pine64 and FXP).

Il utilise ses propres applications. Certaines applications Android peuvent être exécutées sur Ubuntu Touch en utilisant des applications qui permettent d’exécuter des applications Android en conteneur sur les systèmes Linux sans avoir besoin d’un système d’exploitation Android complet. Il y aurait environ 200 000 à 300 000 utilisateurs d’Ubuntu Touch.

* Sailfish OS

https://sailfishos.org/

« Sailfish OS est une alternative européenne basée sur Linux aux systèmes d’exploitation mobiles dominants, et le seul système d’exploitation mobile offrant un modèle de licence exclusif pour les implémentations locales ».

Il est compatible avec les appareils suivants :
https://docs.sailfishos.org/Support/Supported_Devices/.

Il utilise son propre magasin d’applications, Jolla Store. Il y aurait environ 80 000 à 120 000 utilisateurs, essentiellement des développeurs.

* PostmarketOS

https://postmarketos.org/

« PostmarketOS développe des logiciels gratuits et open-source pour prolonger la vie de l'électronique grand public. En permettant aux gens d'avoir le plein contrôle de leurs appareils, nous faisons la promotion d'une société plus saine et plus durable »

Il est compatible avec les appareils suivants : https://wiki.postmarketos.org/wiki/Devices. Il y aurait environ 1 000 utilisateurs.

* Mobian

https://mobian-project.org/

« Un dérivé de Debian pour les appareils mobiles ».

Il est compatible avec les appareils suivants : https://wiki.debian.org/Mobian/Devices, surtout des smartphones Pine64 et OnePlus. Il y aurait environ 2 000 à 5 000 utilisateurs.

* Plasma Mobile

https://plasma-mobile.org

« Un écosystème pour les téléphones qui respecte la confidentialité, les logiciels gratuits et sécurisés ».

Plasma Mobile peut être installé sur des distributions Linux telles que PostmarketOS ou Mobian.

Il y aurait peu d'utilisateurs de Plasma Mobile, environ 1 000, car c'est un projet à ses débuts.

* PureOS

https://www.pureos.net/

« Un système d'exploitation entièrement convergent, convivial, sécurisé et respectueux de la liberté pour votre utilisation quotidienne. Avec PureOS, vous êtes le seul à contrôler votre vie numérique ».

PureOS est officiellement compatible uniquement avec le smartphone Librem 5 fabriqué par Purism.

Il y a quelques projets communautaires pour le rendre compatible des PinePhone et de Mobian sur quelques Nokia. Purism a livré environ 20 000 Librem 5 avec PureOS.

→ À l'échelle mondiale, les utilisateurs alternatifs de distributions Linux sur les smartphones sont de 300 000 à 450 000.

Distributions Android alternatives :

Ces distributions peuvent utiliser des applications de leur propre magasin d'applications, de magasins alternatifs, et peuvent utiliser les applications Google Play via Aurora ou via une version en bac à sable de Google Play Store (pour GrapheneOS uniquement).

* /e/OS

https://e.foundation/e-os/

« /e/OS est un écosystème mobile complet, entièrement dé-Googlé ».

/e/OS est un système d'exploitation mobile open source associé à des applications soigneusement sélectionnées. Ils forment un système interne compatible avec la confidentialité pour votre smartphone. Et ce ne sont pas seulement les affirmations : l'open source signifie une confidentialité vérifiable.

/e/OS a reçu une reconnaissance académique de chercheurs de l'Université d'Édimbourg et du Trinity College de Dublin.

/e/OS aurait pu se concentrer sur un système d'exploitation, mais les applications et les services en ligne sont également des éléments cruciaux de l'expérience quotidienne.

Ces services en ligne, y compris le moteur de recherche, la plate-forme de messagerie, le stockage cloud et d'autres outils en ligne, créent un environnement unique et amélioré de confidentialité.

Il est compatible avec les appareils suivants : https://doc.e.foundation/devices. Murena vend quelques smartphones avec /e/OS préinstallé.

Les applications sont installées depuis l'App Lounge : l'App Lounge est la deuxième itération du magasin d'applications intégré à /e/OS. Il permet à chacun d'accéder à des millions d'applications directement à partir de l'écran d'accueil de son téléphone.

Il combine des applications Android courantes, des applications open source et même des applications Web progressives dans un seul référentiel. C'est le seul magasin d'applications qui le fait aujourd'hui. Vous n'avez pas besoin de vous connecter à un compte pour télécharger des applications. Il y aurait environ 200 000 utilisateurs d'/e/OS.

* LineageOS

https://lineageos.org/

« Un système d'exploitation gratuit et open source pour divers appareils, basé sur la plate-forme mobile Android ».

Il est le successeur de CyanogenMod.

Il est compatible avec les appareils suivants : https://wiki.lineageos.org/devices/.

Il comprend un ensemble d'applications open source. Les applications Google ne sont pas intégrées à LineageOS mais peuvent être téléchargées séparément. Il y aurait environ 1 800 000 utilisateurs de LineageOS.

* iodéOS

https://iode.tech/fr/iodeos/

« Android sans Google.

iodéOS intègre un système d'exploitation Android débarrassé des mouchards Google. Une part significative des fuites de données intervient en amont des applications, contrôler ces dernières ne suffit pas.

iodéOS est basé sur LineageOS, qui étend les fonctionnalités et la durée de vie des téléphones mobiles et tablettes de plus de 20 fabricants différents grâce à une communauté open source de

contributeurs du monde entier. L'interface Trust vous aidera à comprendre la sécurité de votre appareil et à vous prévenir des menaces éventuelles ».

iodéOS est compatible des appareils suivants :

https://iode.tech/fr/appareils-pris-en-charge-officiellement-par-iodeos/

Des smartphones sur lesquels iodéOS est installé sont en vente sur le site : https://shop.iode.tech/fr/

* GrapheneOS

https://grapheneos.org/

« Le système d'exploitation mobile privé et sécurisé compatible des applications Android. Développé comme un projet open source à but non lucratif ».

Il est compatible avec les appareils suivants : https://grapheneos.org/faq#supported-devices, exclusivement des Google Pixel, en raison des exigences matérielles de sécurité de GrapheneOS.

GrapheneOS est une version à sécurité durcie d'Android, libérée de Google, avec son propre magasin d'applications. Google Play Store peut être installé éventuellement dans un bac à sable.

GrapheneOS fournit probablement la meilleure compatibilité avec les applications Google Play Store. Il y aurait environ 60 000 utilisateurs de GrapheneOS.

* CalyxOS et Pixel Experience ne sont plus maintenus.

→ À l'échelle mondiale, en tenant compte des utilisateurs de CalyxOs et de Pixel Experience, il y aurait environ 2 600 000 utilisateurs de distributions Android alternatives.

* Huawei

https://consumer.huawei.com

Le cas de Huawei est particulier : Huawei vend des smartphones Android, sans aucun accès aux logiciels de Google.

Les smartphones Huawei n'ont pas accès au Google Play Store ni aux applications Google ; ils ont accès à leur propre boutique d'applications et à des magasins alternatifs (y compris les applications Aurora pour Play Store).

D'une certaine manière, les utilisateurs de smartphones Huawei sont libérés du pistage par Google, mais il est remplacé par celui de Huawei !

* XDA Developers

https://xdaforums.com/

Sur les forums XDA Developers, vous pouvez trouver des ROM personnalisées pour certains appareils Android.

3.3) Utilisation des smartphones Android du commerce

La plupart des utilisateurs d'Android utilisent des appareils Android avec le système d'exploitation fourni par le fabricant (Android 14, 15, 16…) et son ajustement.

Cependant, l'utilisateur peut configurer son appareil Android commercial afin d'améliorer sa sécurité, sa confidentialité et même avoir un certain anonymat.

Protection contre les logiciels malveillants, les pisteurs et la publicité.

Cette partie s'applique également aux smartphones Android avec une distribution Android alternative.

Nous parlons ici de logiciels malveillants sur Internet (sites malicieux), pas des logiciels malveillants que vous pouvez installer depuis les magasins. Les meilleurs résolveurs DNS filtrant concernant la protection des logiciels malveillants sont « protective.joindns4.eu » et d'autres résolveurs DNS de filtrage de la famille joindns4.eu. Ils utlisent une base de données de plus de vingt millions de sites Web malveillants. Cette base de données est continuellement mise à jour, l'IA est utilisée pour analyser le comportement des sites Web.

1re méthode : utilisation d'un résolveur DNS de filtrant et du navigateur DuckDuckgo.

Choisissez le résolveur DNS filtrant que vous voulez, voir Résolveurs DNS filtrants, et entrez son nom DoT dans le paramètre DNS privé qui se trouve trouvé dans les paramètres / Internet et réseau.

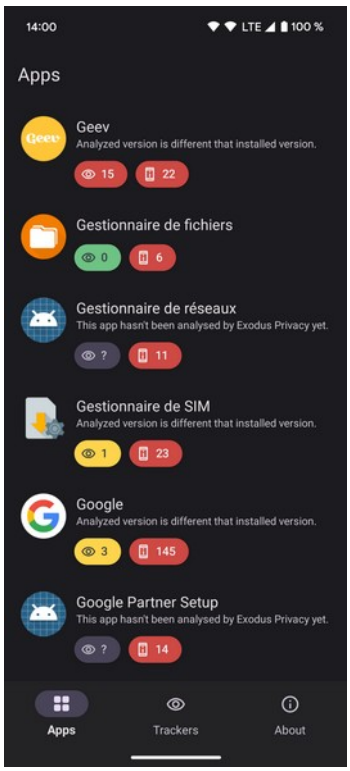
Exemples :

> « noads.joindns4.eu » pour le résolveur DNS à sécurité renforcée et blocage des publicités de DNS4EU,
>
> « 1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com » pour un résolveur DNS Rethink avec les filtres Security Full et Privacy Agressive,
>
> « xxxxxxxx.dot.ublockdns.com », avec les listes de filtrage et les résolveurs DNS de votre choix.

Le filtrage sera fait à l'échelle du système, pour toutes les applications installées et le système d'exploitation.

Installez le navigateur DuckDuckgo depuis Google Play Store. DuckDuckGo Browser est un mauvais navigateur (pas d'extension, basé sur WebView et qui révèle l'adresse IP interne via une fuite WebRTC), mais nous l'utiliserons juste pour ajouter une couche de filtrage supplémentaire des pisteurs des applications installées sur l'appareil, en utilisant sa protection contre le pistage par les applications. Pour plus d'information, voir https://duckduckgo.com/duckduckgo-help-pages/p-app-tracking-protection/what-is-app-tracking-protection.

Le pistage par les applications est différent du pistage habituel qui se produit lors de l'utilisation d'un navigateur ; les pisteurs sont spécifiques. Vous pouvez installer sur votre smartphone Android l'application Exodus Privacy ; elle analysera les applications installées sur votre smartphone et téléchargera les rapports donnant, pour chaque application, les pisteurs utilisés par l'application et la liste des autorisations requises par l'application.



En couplant à la fois le filtrage par un résolveur DNS et la protection de DuckDuckGo contre le pistage par les applications, vous pouvez protéger votre appareil Android contre les logiciels malveillants, les publicités et le pistage.

2e méthode : utilisation de personalDNSfilter

personalDNSfilter est une application qui peut être téléchargée depuis Google Play Store et peut être utilisée sur un périphérique Android standard, sans mode racine.

Elle combine l'utilisation du résolveur DNS de votre choix, à l'aide d'adresses IPv4 ou IPv6 (cela exclut les résolveurs DNS Rethink et uBlockDNS), avec un ensemble de filtres, acceptant deux syntaxes : fichier « hosts » ou filtres DNS. Vous pouvez choisir un ou plusieurs des filtres préexistants ou ajouter un filtre de votre choix.

Plus d'informations, voir https://www.zenz-solutions.de/personaldnsfilter-wp/.

J'utilise le résolveur DNS « noads.joindns4.eu », en mode DoT, avec les adresses IP suivantes :

86.54.11.13

86.54.11.213

2a13:1001::86:54:11:13

2a13:1001::86:54:11:213

Voici les listes de filtres que j'utilise (maliciels, publicités, pisteurs et réseaux sociaux) :

Publicités :
https://v.firebog.net/hosts/AdguardDNS.txt;
https://v.firebog.net/hosts/Easylist.txt;

https://raw.githubusercontent.com/lassekongo83/Frellwits-filter-lists/master/Frellwits-Swedish-Hosts-File.txt.
Maliciels :
https://raw.githubusercontent.com/greatis/Anti-WebMiner/master/hosts;
https://raw.githubusercontent.com/hoshsadiq/adblock-nocoin-list/master/hosts.txt;
https://malware-filter.gitlab.io/malware-filter/urlhaus-filter-hosts.txt;
https://urlhaus.abuse.ch/downloads/hostfile/;
https://raw.githubusercontent.com/FadeMind/hosts.extras/master/add.Spam/hosts;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/rpz/tif.mini.txt;
https://raw.githubusercontent.com/davidonzo/Threat-Intel/master/lists/latestdomains.piHole.txt.
Pisteurs :
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.amazon.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.apple.txt;
https://v.firebog.net/hosts/Easyprivacy.txt;
https://hostfiles.frogeye.fr/multiparty-trackers-hosts.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.huawei.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.winoffice.txt;
https://raw.githubusercontent.com/mullvad/dns-blocklists/refs/heads/main/files/tracker;
https://raw.githubusercontent.com/notracking/hosts-blocklists/master/hostnames.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.oppo-realme.txt;
https://gitlab.com/quidsup/notrack-blocklists/-/raw/master/trackers.hosts;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.tiktok.extended.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.vivo.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.xiaomi.txt.
Filtres multiples :
(Publicités, Affiliation, Pistage, Métriques, Télémétrie, Hameçonnage, Maliciels, Arnaque, Faux, Voleurs de cryptomonnaies et autres mer..s).
https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts;
https://big.oisd.nl/domainswild2;
https://raw.githubusercontent.com/hagezi/dns-blocklists/main/wildcard/pro-onlydomains.txt.
Réseaux Sociaux :
(L'utilisation de cette liste empêchera l'utilisation de Facebook, Instagram, Pinterest, Snapchat, Tiktok, X etc., mais permettra l'utilisation de WhatsAppp).
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/wildcard/social-onlydomains.txt.

Avec personalDNSfilter, pas besoin du navigateur DuckDuckgo ; de plus, il comprend la possibilité de mettre en liste blanche certains sites Web (inclus dans les filtres) auxquels vous voudriez vous connecter et d'ajouter manuellement certains sites Web que vous voudriez filtrer, ainsi que de mettre des applications en liste blanche (pour lesquelles les filtres ne s'appliqueront pas).

Libération partielle de Google

Ceci ne s'applique pas aux smartphones avec une distribution alternative d'Android.

J’ai désinstallé ou désactivé (lorsque la désinstallation est impossible) toutes les applications Google que je n’utilise pas :

- Android Auto,
- Gemini,
- Gmail (remplacé par Thunderbird),
- Google,
- Google Assistant,
- Google Chrome (remplacé par Firefox),
- Google Docs (remplacé par Collabora Office),
- Google Fit,
- Google Maps (peut être utilisé de manière plus confidentielle dans un navigateur),
- Google Meet (peut être utilisé de manière plus confidentielle dans un navigateur),
- Google News (peut être utilisé de manière plus confidentielle dans un navigateur),
- Google TV,
- Google Voice Recognition and Synthesis (gardez-la activée si vous avez besoin de la synthèse vocale et supprimez l’autorisation d’accès au microphone),
- Notes Keep,
- YouTube (peut être utilisé de manière plus confidentielle dans un navigateur),
- YouTube Music (remplacé par VLC).

Choix du navigateur

Il existe deux grandes familles de navigateurs disponibles pour Android. Ils peuvent être installés depuis F-Droid, FFUpdater (dans la boutique F-Droid) ou depuis Google Play Store pour certains :
– Firefox et navigateurs basés sur Firefox :
Versions stables :

- Firefox, orienté confidentialité, nombreuses extensions disponibles,
- Fennec F-Droid, identique à Firefox, sans télémétrie,
- Firefox Focus, fonctionnalités réduites,
- Firefox Klar, identique à Firefox Focus, sans télémétrie,
- Navigateur Tor, navigation anonyme via le réseau Tor.

Versions expérimentales, moins testées, moins stables :

- Firefox Beta, pour tester la prochaine version de Firefox,
- Firefox Nightly, pour les développeurs, pour tester les futures fonctionnalités,
- IronFox, il emprunte certaines fonctionnalités à Firefox Nightly et utilise le code de l’ancien Mull Browser, confidentialité améliorée,
- Iceraven, offrant plus d’options et plus de possibilités de personnalisation.

– Chromium et navigateurs basés sur Chromium :
La famille de navigateurs basés sur Chromium est réputée pour être plus sécurisée que ceux basés sur Firefox. Cependant, ils sont généralement moins respectueux de la confidentialité.
Versions stables :

- Google Chrome est le pire navigateur en termes de confidentialité, lié aux serveurs de Google, sans extension,
- Chromium est toujours lié aux serveurs de Google, mais moins que Chrome,

- Brave Browser, censé protéger la vie privée des utilisateurs, mais livré avec ses propres publicités,
- Vivaldi Browser, axé sur la confidentialité et avec bloqueur de publicités, mais pas entièrement Open Source,
- F-Droid Privacy Browser, axé sur la confidentialité, mais bloqueur de publicités limité,
- Duck Duck Go Browser, axé sur la confidentialité mais avec fuite WebRTC, avec anti-pistage mais sans bloqueur de publicité, pas d'extension.

Version expérimentale, moins testée, moins stable :

- Cromite, sécurité et confidentialité améliorées, utilisant le code de l'ancien Bromite, bloqueur de publicités intégrées et dispositions anti-empreintes digitales, pas de cast, pas de lecture de vidéos DRM, pas d'extension.

Le navigateur le plus réputé en termes de sécurité est Vanadium, mais il n'est disponible que dans GrapheneOS puisqu'il utilise certaines fonctionnalités de sécurité de sa distribution.

Un zoom sur Firefox et Cromite

Firefox pour Android est mon navigateur par défaut, il remplace Google Chrome. Il est disponible sur Google Play Store.

Paramètres :

- « about:config » existe, mais est caché, comme pour Firefox; on y accède par « chrome://geckoview/content/config.xhtml » ; faites-en un raccourci.
- Vérifiez que « fission.autostart » et « fission.autostart.session » ont pour valeur « true ».

Apportez les modifications suivantes dans « about:config » ou vérifiez qu'elles sont déjà là :

- « browser.cache.disk.enable » à mettre sur « false », pour désactiver la mise en cache disque.
- « webgl.enable-debug-renderer-info » à mettre sur « false », pour éviter que le pilote graphique soit exposé.
- « media.peerconnection.enabled » à mettre sur « false », pour désactiver la fuite par WebRTC.
- « javascript.options.baselinejit » à mettre sur « false », pour désactiver la compilation JavaScript en temps réel, cela réduit la surface d'attaque de JavaScript.
- « network.idn_show_punycode » à mettre sur « true », pour être protégé contre les attaques homographes IDN, (les URL avec des caractères non latins seront affichées sous forme de punycode).
- « network.captive-portal-service.enabled » à mettre sur « false », pour désactiver la télémétrie de Firefox.
- « captivedetect.canonicalURL », remplacer l'adresse http par une chaîne vide de caractères, pour désactiver la télémétrie de Firefox,
- « dom.fs.enabled » à mettre sur false, pour éviter l'écriture OPFS sur SSD et le pistage correspondant par empreintes digitales.

J'ai installé les extensions suivantes :

- « Canvas Blocker », protection contre le pistage par empreintes du navigateur.
- « CSS Exfil Protection », empêche la fuite de données via les feuilles de styles.
- « Dark Reader », permet d'afficher les pages avec des caractères blancs sur fond noir (c'est une question de goût).

- « DuckDuckGo Search and Tracker Protection », protection de la confidentialité, elle installe la recherche DuckDuckGo comme page d'accueil, le moteur de recherche DuckDuckGo par défaut et l'extension « DuckDuckGo Privacy Essentials ».
- « Privacy Badger », protection contre le pistage.
- « Font Fingerprint Defender », protection contre le pistage par empreintes du navigateur.
- « uBlock Origin », l'un des meilleurs filtres de la publicité, contre le pistage et contre les maliciels est préinstallé.
- « NoScript Security Suite », qui permet de n'activer javascript que sur les sites de confiance.

Notez que toutes les extensions de Firefox ne sont pas disponibles pour la version Android de Firefox. Cependant, l'utilisation du mode de débogage (tapez cinq fois sur les paramètres / à propos de Firefox) permet d'installer n'importe quelle extension à partir d'un fichier.

Vous souhaiterez peut-être installer un autre navigateur que Firefox : Cromite est un fork de Chromium, basé sur l'ancien Bromite, il s'agit d'une version renforcée en matière de confidentialité de Chromium, avec sa propre capacité de filtrage basée sur AdBlock Plus, offrant toujours la sécurité totale de Chromium. Voir : https://github.com/uazo/cromite.
Il n'est pas disponible sur Google Play Store ; pour l'installer, vous devez d'abord télécharger et installer le magasin F-Droid, à partir de https://f-droid.org/. Ensuite, pour installer Cromite, ajoutez le référentiel suivant à F-Droid :
https://www.cromite.org/fdroid/repo/?fingerprint=49F37E74DEE483DCA2B991334FB5A0200787430D0B5F9A783DD5F13695E9517B
puis recherchez Cromite dans F-Droid et installez-le. Notez que Cromite est maintenu par une très petite équipe et pourrait disparaître sans préavis, comme Bromite ; vérifiez qu'il est mis à jour régulièrement.

Voici une comparaison entre Firefox et Cromite sur les aspects sécurité et confidentialité

Fonctionnalité	**Firefox**	**Cromite**
Bac à sable	Basique	Renforcé (seccomp-bpf dans l'application)
Isolation des autres applications	Basique	Renforcé (1)
Isolation des processus internes	Oui, Fission (2)	Oui
Protection contre le suivi	Stricte (3)	Moyenne (4)
Télémétrie	Oui (mais désactivable)	Aucune
Extensions	Oui	Non (5)
Restriction d'accès au réseau local	En service (6)	En service (6)

[NB :
(1) : Cromite utilise la fonctionnalité « android:isolatedProcess="true" » dans son manifeste ; il est ainsi exécuté selon un processus spécial. La seule communication avec lui se fait via l'API Service.
(2) : Fission est activée dans Firefox pour Android depuis la version 147.0.

(3) : La protection stricte contre le suivi est disponible, Google Safe Browsing est disponible et on peut installer des extensions comme uBlock Origin, Privacy Badger, DuckDuckGo Search & Tracker Protection, Canvas Blocker, Font Fingerprint Defender.
(4) : Cromite inclut des protections contre les empreintes numériques et un bloqueur de publicité intégré dérivé d'Adblock Plus, Google Safe Browsing n'est pas disponible.
(5) : L'absence d'extensions dans Cromite ne permet pas d'installer uBlock Origin, Privacy Badger, DuckDuckGo Privacy Essentials, Canvas Blocker, Font Fingerprint Defender, qui ont un impact sur le pistage et la confidentialté ; ni NoScript, qui a un impact sur la sécurité ; ni CSS Exfil Protection, qui a un impact sur la confidentialité.
(6) : Sans cette restriction, les sites Web publics peuvent sonder le réseau local d'un utilisateur et effectuer des attaques CSRF contre les appareils locaux vulnérables, et abusent généralement du navigateur en usurpant les droits de l'utilisateur qui a accès au réseau local ou au logiciel sur sa machine locale. Firefox est conforme à la spécification d'accès au réseau local, https://wicg.github.io/local-network-access/, à partir de la version 149, tandis que les navigateurs basés sur Chromium s'y conforment à partir de la version 152.]

Il est possible d'utiliser Firefox avec une isolation supplémentaire, dans un profil de travail :

- Installez un magasin F-Droid, à partir de https://f-droid.org/.
- Depuis F-Droid, installez Shelter.
- Lancez Shelter ; une fois le profil de travail créé, désactivez dans le profil de travail les applications Google que vous n'utilisez pas.
- Lors de la création du profil de travail, Play Store a été cloné.
- Depuis Play Store dans le profil de travail, installez Firefox.

F-Droid dans votre profil personnel tiendra à jour Shelter. Play Store dans le profil de travail tiendra à jour Firefox. Firefox fonctionnera dans le profil de travail, isolé des autres applications fonctionnant dans le profil personnel.

Autres précautions

- Activez la localisation, NFC, Bluetooth, Wi-Fi uniquement lorsque vous en avez besoin.
- Ne vous connectez jamais à un spot Wi-Fi public.
- Pour chaque application installée, paramétrez ses notifications, autorisations, utilisation de la batterie ; révoquez les autorisations inutiles ou excessives pour les fonctionnalités de l'application.
- Utilisez l'application « System Manager » pour définir le « mode d'économie d'énergie », il empêchera la plupart des applications de fonctionner en arrière-plan.
- Si le réglage est disponible (Android 14 et ultérieur), désactivez la 2G.
- Lorsque c'est possible, préférez utiliser le navigateur qu'une application dédiée (exemple : connectez-vous à Facebook avec Firefox, n'utilisez pas l'application Facebook).
- Gardez votre système Android, Play Protect et vos applications à jour.
- Il est recommandé d'arrêter et de redémarrer périodiquement les appareils Android afin de supprimer les logiciels malveillants qui persisteraient dans la mémoire.
- Utilisez un gestionnaire de mots de passe pour stocker localement tous les mots de passe, protégez son accès avec un mot de passe fort.

- Utilisez uniquement des communications entièrement chiffrées de bout en bout (n'utilisez plus les SMS ; utilisez RCS entre appareils Android ; à la date d'avril 2026, n'utilisez pas RCS entre appareils Android et iPhones ; utilisez une application de messagerie entièrement chiffrée de bout en bout entre appareils Android et iPhones, voir « Anonymat » ci-dessous).
- Activez la navigation sécurisée d'Android : lorsque vous avez supprimé Google Chrome et d'autres applications Google, la liste des applications bénéficiant de la navigation sécurisée est courte, mais l'activer empêchera les logiciels malveillants et l'hameçonnage pour ces applications. Les URL que vous demandez sont envoyées sous forme de sceaux cryptograhiques aux serveurs de Google. Notez que la navigation sécurisée est par ailleurs incluse dans Firefox, avec une vérification locale.
- Activez Google Play Protect.
- Lorsque vous achetez un nouveau smartphone, optez pour la dernière version matérielle du fabricant, le matériel plus récent intègre souvent des fonctionnalités de sécurité critiques que le matériel plus ancien ne peut pas prendre en charge. Sans la version la plus récente du matériel, les mises à jour logicielles à elles seules ne fourniront pas le maximum d'avantages en matière de sécurité.

VPN

Il est possible d'utiliser un VPN dans les appareils Android. Une fois installé, la connexion VPN peut être définie comme permanente dans Paramètres / Internet et réseau. L'utilisation d'un VPN est obligatoire avec certains FAI qui utilisent l'adresse IP pour pister les utilisateurs et leur attribuer un identifiant unique pour publicités personnalisées en utilisant Utiq (Deutsche Telekom, Telefónica, Vodafone, Orange, Bouygues Telecom, SFR, Free…).

Utilisez un VPN sans aucune journalisation, tel que Proton VPN ou Mullvad VPN.

Notez que l'utilisation d'un VPN empêche l'utilisation du navigateur DuckDuckgo et celle de personalDNSfilter ; bien qu'ils ne soient pas des VPN, ils utilisent le réglage VPN d'Android.

Il est cependant possible d'utiliser un VPN avec un filtre DNS. Trois méthodes :
Avec Proton VPN :

- Installez l'application « Proton VPN » depuis Google Play Store et lancez l'application en mode « invité » ou connectez-vous en mode « gratuit ».
- Dans les paramètres réseau et internet d'Android, saisissez un nom de résolveur DNS filtrant, par exemple « xxxxxxxx.dot.ublockdns.com ».
- La connexion à internet se fera via ProtonVPN, et les requêtes DNS seront envoyées via Proton VPN en mode sécurisé au résolveur DNS filtrant.

Avec Rethink :

- Installez l'application « Rethink: DNS + Pare-feu + VPN » depuis Google Play Store.
- Lancez l'application et configurez les filtres.
- Téléchargez une configuration Wireguard pour votre VPN. Par exemple, pour Proton VPN, connectez-vous à https://account.protonvpn.com/downloads et téléchargez une configuration VPN.

- Importez votre configuration VPN dans l'application Rethink.

Avec Wireguard :

- Installez l'application « Wireguard » depuis Google Play Store.
- Téléchargez une configuration Wireguard pour votre VPN. Par exemple, pour Proton VPN, connectez-vous à https://account.protonvpn.com/downloads et téléchargez une configuration VPN.
- Lancez l'application et importez la configuration.
- Dans l'application, changez les adresses des résolveurs DNS, mettez celles des résolveurs DNS filtrants de votre choix.

[NB : il n'est plus possible d'utiliser « OpenVPN for personalDNSfilter » en conjonction avec « personalDNSfilter », cette application de VPN, ancienne, est obsolète.]

Anonymat

Le navigateur Tor Browser est disponible dans le Play Store ; utilisez les mêmes paramètres que pour Firefox et utilisez l'extension intégrée NoScript Security Suite. Cependant, Tor Browser pour Android est actuellement (le 8 avril 2026) basé sur Firefox 140.7 esr et il ne disposera de Fission que lorsqu'il sera basé sur Firefox 147 ou version ultérieure. Pour vérifier si Fission est disponible :

- « about:config » existe, mais est caché, comme pour Firefox; on y accède par « chrome://geckoview/content/config.xhtml » ; faites-en un raccourci.
- Vérifiez que « fission.autostart » et « fission.autostart.session » ont pour valeur « true ».

Vous pouvez installer des extensions dans Tor Browser en utilisant le mode de débogage (tapez cinq fois sur les paramètres / à propos de Tor Browser) qui permet d'installer n'importe quelle extension à partir d'un fichier. Installez les mêmes extensions que pour Firefox ou un jeu réduit (augmenter le nombre d'extensions augmente le pistage par empreintes du navigateur).

Deux méthodes pour une sécurité renforcée :
– Utilisez Tor Browser avec une isolation supplémentaire, dans un profil de travail :

- Installez un magasin F-Droid, à partir de https://f-droid.org/.
- Depuis F-Droid, installez Shelter.
- Lancez Shelter ; une fois le profil de travail créé, désactivez dans le profil de travail les applications Google que vous n'utilisez pas.
- Lors de la création du profil de travail, Play Store a été cloné.
- Depuis Play Store dans le profil de travail, installez TorBrowser.

F-Droid dans votre profil personnel tiendra à jour Shelter. Play Store dans le profil de travail tiendra à jour Tor Browser. Tor Browser fonctionnera dans le profil de travail, isolé des autres applications fonctionnant dans le profil personnel.
– Ou utilisez Orbot et lancez avec Orbot le navigateur de votre choix, Firefox ou Cromite.
Voici comment lancer Firefox avec Tor :

- Installez Orbot.
- Lancez Orbot en mode utilisateur avancé.
- Dans la barre d'adresse de Firefox saisissez « chrome://geckoview/content/config.xhtml ».

- Modifiez les valeurs suivantes :
  « network.proxy.socks », valeur « 127.0.0.1 »,
  « network.proxy.socks_port », valeur « 9050 »,
  « network.proxy.type », valeur « 1 ».
- Fermez « about:config ».
- Vérifiez que Firefox utilise bien Tor : https://check.torproject.org/.

Pour revenir au mode normal, sans Tor, de Firefox, saisissez
« chrome://geckoview/content/config.xhtml » et changez la valeur de « network.proxy.type », remettez-la à « 0 ».
Plusieurs applications de messagerie offrent l'anonymat et le chiffrement complet de bout en bout. Évitez WhatsApp (source non divulguée), Telegram (chiffré jusqu'aux serveurs par défaut, le mode « Secret Chat » doit être activé pour avoir un chiffrement de bout en bout), préférez Signal ou Olvid.

4. iPhones

4.1) Introduction aux iPhones

Les iPhones sont exclusivement fabriqués par Apple; leur système d'exploitation, iOS, est du genre « source non divulguée », et toutes les applications sont préinstallées par Apple ou proviennent d'Apple App Store.

L'UE a demandé à Apple d'ouvrir ses smartphones aux magasins alternatifs, menaçant Apple de centaines de millions de dollars d'amendes ; Apple a finalement accepté et a supprimé toute difficulté d'utiliser un autre magasin depuis iOS 18.6. Bien entendu, la sécurité des applications installées depuis un autre magasin n'est pas gérée / garantie par Apple.

La sécurité est ainsi sous le contrôle strict d'Apple. Les failles de sécurité sont peu connues. Le programme de récompenses d'Apple, pour les chercheurs qui trouvent des failles de sécurité, est récent (2020) et limité à des récompenses maximales de 500 000 USD ; certains chercheurs préfèrent toujours vendre leurs découvertes à une entreprise israélienne (Pegasus) qui paie pour cela et crée des programmes permettant d'espionner iOS, programmes vendus à un coût très élevé aux gouvernements. La sécurité globale semble très bonne.

Les applications sont fortement isolées, au point qu'elles ne peuvent rien partager (si vous souhaitez utiliser Apple Music et VLC pour écouter de la musique, vous devez copier votre musique dans les répertoires des deux applications).

iOS a une certaine protection contre le suivi, la protection contre le pistage croisé par les applications n'est qu'un paramètre à sélectionner, et Safari, le navigateur Web, comprend une certaine protection contre le pistage. Les publicités semblent s'afficher moins agressivement dans les applications que dans leurs versions Android.

4.2) Protection contre les maliciels, la publicité et le pistage dans iOS

Il n'y a qu'une seule méthode qui fonctionne à l'échelle du système : l'utilisation d'un résolveur DNS filtrant (voir Résolveurs DNS filtrants).

Il n’y a pas d’équivalent à personalDNSfilter pour iOS, et le navigateur DuckDuckgo pour iOS ne peut pas fonctionner comme une protection contre le pistage par les applications.

Les meilleurs résolveurs DNS filtrant concernant la protection des logiciels malveillants sont « protective.joindns4.eu » et d’autres résolveurs DNS de filtrage de la famille joindns4.eu. Ils utilisent une base de données de plus de vingt millions de sites Web malveillants. Cette base de données est continuellement mise à jour, l’IA est utilisée pour analyser le comportement des sites Web.

Si vous souhaitez utiliser un résolveur DNS filtrant les logiciels malveillants et les publicités, vous devez utiliser :

- Un des résolveurs DNS de DNS4EU, « noads.joindns4.eu », ou « child-noads.joindns4.eu ».
- Une version personnalisée du résolveur DNS Rethink DNS, par exemple avec les filtres Security Full et Privacy Aggressive :

  « 1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com ».
- Une version personnalisée du résolveur uBlockDNS, par exemple :

  « xxxxxxxx.dot.ublockdns.com ».

Afin de définir un résolveur DNS dans les appareils iOS, vous avez besoin d’un profil DNS ; un tel profil DNS peut être téléchargé pour DNS4EU et uBlockDNS à partir de leurs sites Web (voir les liens dans Résolveurs DNS filtrants).

Rethink DNS n’offre pas une telle possibilité. Vous pouvez générer un profil DNS à partir du créateur de profil DNS sécurisé, https://dns.notjakob.com/.

Une fois que vous avez le profil dont vous avez besoin, vous l’importez dans votre appareil iOS (envoyez-le par courriel, installez-le dans les paramètres généraux / VPN et gestion des appareils et validez-le) ; il sera actif dans la section « Restrictions et Proxy ».

Navigateur : il n’est pas nécessaire d’utiliser un autre navigateur que Safari ; en raison des restrictions d’Apple, Firefox pour iOS est très médiocre, basé sur WebKit (le même moteur de rendu que Safari), et n’a pas d’extension. Le seul intérêt est pour Firefox Focus, qui peut être utilisé comme navigateur avec des fonctionnalités « oubli rapide » et « anti-pistage » ; de plus, il peut agir comme un bloqueur de contenu pour Safari.

Vous pouvez installer l’extension « UBlock Origin Lite » pour Safari ; une fois installée, donnez-lui les autorisations nécessaires, définissez le niveau de protection et sélectionnez les listes de filtres.

Vous pouvez compléter les fonctionnalités anti-pistage de Safari à l’aide de Firefox Focus et utiliser une version gratuite d’Adguard ou d’AdBlock Plus comme bloqueurs de contenu supplémentaires. Pour éviter l’écriture OPFS sur SSD et le pistage correspondant par empreintes digitales, utilisez Safari en mode privé (ouvrez un nouvel onglet privé), l’écriture OPFS sera effacée après fermeture de l’onglet privé.

Autres précautions pour iOS

- Il est recommandé d'arrêter et de redémarrer périodiquement les appareils iOS, pour supprimer les maliciels persistant en mémoire.
- Comme pour tout système d'exploitation, il est recommandé de le mettre à jour le plus souvent possible (système iOS et applications), pour les corrections de bogues et les correctifs de sécurité.
- Activez la localisation, Bluetooth et Wi-Fi uniquement lorsque vous en avez besoin.
- Ne vous connectez jamais à un point d'accès Wi-Fi public.
- Pour chaque application installée, paramétrez ses notifications, autorisations ; révoquez les autorisations inutiles ou excessives pour les fonctionnalités de l'application.
- Désactivez Siri, globalement et dans chaque réglage d'application.
- Utilisez le mode économie d'énergie en permanence, il empêche les applications de fonctionner en arrière-plan.
- Mettez en place la protection contre le pistage croisé par les applications.
- Lorsque c'est possible, préférez utiliser le navigateur qu'une application dédiée (exemple : connectez-vous à Facebook avec Safari, n'utilisez pas l'application Facebook).
- Utilisez un gestionnaire de mots de passe pour stocker localement tous les mots de passe, protégez son accès avec un mot de passe fort.
- Utilisez uniquement des communications entièrement chiffrées de bout en bout (utilisez iMessages uniquement entre iPhones ; à la date d'avril 2026, n'utilisez pas RCS entre iPhones et appareils Android ; utilisez une application de messagerie entièrement chiffrée de bout en bout entre iPhones et appareils Android, voir « Anonymat sur iOS » ci-dessous).
- Désactivez le paramètre « Envoyer sous forme de message texte » pour garantir que les messages ne soient pas envoyés sous forme de SMS si iMessage n'est pas disponible (iMessage propose un cryptage de bout en bout entre les utilisateurs Apple uniquement).
- Activez le Lockdown Mode. Ce mode de verrouillage limite strictement certaines applications, sites Web et fonctionnalités (ou rend certaines fonctionnalités indisponibles), réduisant ainsi la surface d'attaque qui pourrait potentiellement être exploitée par les acteurs malveillants.
- Pour des protections supplémentaires inscrivez-vous à Apple iCloud Private Relay (voir le Guide de l'utilisateur iCloud pour les instructions de configuration). Private Relay garantit que les appareils iCloud utilisent des DNS sécurisés, masque les adresses IP et répartit le trafic entre les serveurs contrôlés par Apple et un tiers afin de réduire les chances qu'une seule entité puisse lier le comportement du navigateur à l'identité de l'utilisateur. Remarque : ces avantages sont limités au navigateur Safari.
- Lorsque vous achetez un nouvel iPhone, optez pour la dernière version matérielle ; le matériel plus récent intègre souvent des fonctionnalités de sécurité critiques que le matériel plus ancien ne peut pas prendre en charge. Sans la version la plus récente du matériel, les mises à jour logicielles à elles seules ne fourniront pas une sécurité maximale.

VPN sur iOS

L'utilisation d'un VPN est possible sur iOS. Voir Paramètres généraux / VPN et gestion des appareils. L'utilisation d'un VPN est obligatoire avec certains FAI qui utilisent l'adresse IP pour

pister les utilisateurs et leur attribuer un identifiant unique pour publicités personnalisées en utilisant Utiq (Deutsche Telekom, Telefónica, Vodafone, Orange, Bouygues Telecom, SFR, Free…). Utilisez un VPN sans aucune journalisation, tel que Proton VPN ou Mullvad VPN.

Anonymat sur iOS

Le navigateur Tor Browser n'est pas disponible dans le Play Store, mais vous pouvez utiliser Onion Browser ou Orbot avec Safari (avec une protection de la confidentialité réduite en raison des restrictions d'Apple, qui limitent la mémoire accessible à 50 MB, ce qui empêche de trouver de longs chemins dans le réseau Tor).

Plusieurs applications de messagerie offrent l'anonymat et le chiffrement complet de bout en bout. Évitez WhatsApp (source non divulguée), Telegram (chiffré jusqu'aux serveurs par défaut, le mode « Secret Chat » doit être activé pour avoir un chiffrement de bout en bout), préférez Signal ou Olvid.